Debevoise & Plimpton | Data Blog

CCPA

The State of State Law Cybersecurity Requirements

BY: JEREMY FEIGELSON, AVI GESSER, JOHANNA SKRZYPCZYK, ALEXANDRA P. SWAIN, SUCHITA MANDAVILLI BRUNDAGE AND PARKER EUDY - SEPTEMBER 30, 2021

Almost everyone working in cybersecurity compliance is aware that each U.S. state has its own set of breach notification requirements. What is less known is that many of these states also impose substantive cybersecurity requirements. In this Debevoise Data Blog post, we examine the general cybersecurity obligations under state law, including common themes and recent developments.

History of State Law Cybersecurity Requirements

One of the first states to impose general cybersecurity requirements was California in 2004. That law merely required companies to implement and maintain reasonable security procedures and practices to protect personal information from unauthorized access and use, as well as to require by contract that third parties with whom companies disclose personal information do the same. No further guidance was given as to what those reasonable cybersecurity measures may include. Since then, approximately 23 states and Washington, D.C. have adopted laws with similar cybersecurity requirements (collectively, the "Reasonable Security Laws"). These states are included in a table at the end of this blog post.

In addition, California enacted the California Consumer Privacy Act ("CCPA") in 2018. Although the CCPA does not impose substantive cybersecurity requirements on businesses, it does create a private right of action for individuals impacted by a data breach if the breached company failed to maintain reasonable security procedures and practices. *See* Cal Civ. Code § 1798.150.

Many Reasonable Security Laws offer few examples of specific cybersecurity obligations. For example, Arkansas requires only that businesses implement "reasonable security procedures and practices" and "take all reasonable steps to destroy customer records by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable." Ark. Code Ann. § 4-110-104. Maryland, in addition to requiring "reasonable security procedures and practices," requires businesses to dispose of personal information through methods that are appropriate to the nature of the personal information and to require by contract that third-party service providers do the same. *See* Md. Code Ann. §§ 14-3502(b), 14-3503.

Other Reasonable Security Laws have imposed more detailed and onerous cybersecurity requirements. For example, in 2009, Massachusetts enacted several substantive requirements, including a written comprehensive information security program that contains administrative, technical, and physical controls. *See* 201 Mass. Reg. 17.03. Other states that have enacted similarly comprehensive and detailed cybersecurity requirements include New York, Oregon, and Vermont. In addition, there are 11 states that impose specific cybersecurity obligations but that do not require "reasonable security." These states are included in a table at the end of this blog post.

For all of the Reasonable Security Laws, in order to be subject to a state's requirements, an entity must conduct business in the state or acquire or use the personal information of a resident in the state. Penalties for violations of the statutes include fines for each violation or, in the instance of a breach, fines for each resident whose personal information is compromised, as well as actual damages.

One example of enforcement actions brought under these statutes include a May 2021 settlement agreement between Filters Fast LLC and the New York Attorney General for failures to address known cybersecurity vulnerabilities. The settlement agreement requires the company to develop a comprehensive information security program and to implement cybersecurity safeguards such as encryption, segmentation, penetration testing, a virus protection policy, user authentication policy

and procedures, and proactive management of service providers. Similarly, in May 2018, the Massachusetts Attorney General brought an action against Bombas LLC because the company did not develop a written information security program or undertake annual third-party risk assessments.

The Safe Harbor States

Rather than creating substantive cybersecurity obligations (with penalties for non-compliance), some U.S. states have enacted "safe harbor" cybersecurity statutes (collectively, the "Safe Harbor Laws"), which provide companies that have experienced a data breach with affirmative defenses, or safe harbors from punitive damages, if they are sued following the breach. In Ohio, Utah, and Connecticut, a company that is sued following a data breach can defeat the suit entirely, or have its exposure greatly reduced, if it can show that it has adopted and complied with a written cybersecurity program that provides specific administrative, technical, and physical safeguards and that reasonably conforms with an industry standard framework.

While it's not clear that the Safe Harbor Laws' protection from litigation in a single state provide sufficient incentive to push companies to adopt security measures that they would not have otherwise implemented, they do provide some insight into the types of cybersecurity programs that regulators might view as "reasonable."

Emerging Themes of State Law Cybersecurity Requirements

Taking all these U.S. state substantive cybersecurity measures together, below are some examples of what is emerging as "reasonable security" under U.S. state laws. What follows are the generally applicable cybersecurity requirements. For companies operating in industries like finance, insurance, and healthcare, both federal and state laws provide additional guidance on what is expected for "reasonable" security.

1. **Compliance with an Industry Framework.** For businesses seeking to raise an affirmative defense under one of the Safe Harbor Laws, the business must implement and comply with an industry standard framework, such as the frameworks published by the National Institute of Standards of Technology (NIST), the Federal Risk and Management Program (FedRAMP), the Center for Internet Security (CIS), and the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC).
2. **Adoption of Administrative, Physical, and Technical Safeguards.** The obligations prescribed by the Reasonable Security Laws vary in specificity, but one or more of the Reasonable Security Laws require companies operating in a particular state to adopt the following administrative, technical, and physical safeguards for the protection of personal information:

- **Secure record disposal** — ensuring that policies and procedures address proper disposal of records containing personal information;
- **Third-party risk assessment** — conducting sufficient due diligence on third parties with access to personal information;
- **Responsible personnel designation** — designating an employee responsible for the company's data security program;
- **Security training for employees** — providing data security training for employees with access to personal information;
- **Limit employee access to personal information** — implementing policies and procedures to ensure employee compliance with the company's security program, including limiting and/or monitoring access to personal information;
- **Risk-based security self assessment** — conducting a risk-based assessment of the company's security posture;
- **Security detection and/or protection means** — implementing methods to detect and/or protect systems from security threats;
- **Security patching and updates** — maintaining procedures to implement security patches and other updates;
- **Secure user authentication and controls** — implementing procedures to securely authenticate user access to company systems;
- **Encryption for record transmittal and/or storage on portable devices** — encrypting personal information, both in transit and at rest (particularly on devices such as laptops or other portable devices);
- **Management involvement** — informing and updating management on the company's data security program; and
- **Description of security procedures within business's policies** — ensuring security procedures are formally maintained as part of the company's policies and procedures.

3. **Compliance with Other Regulations.** Some states provide that compliance with the cybersecurity requirements of other laws and regulations of that state or the federal government is sufficient. For example, in New York, a business can establish compliance if it is subject to and compliant with 23 NYCRR Part 500 or with "any other data security rules and regulations" of the federal or New York State governments. N.Y. Gen. Bus. Law § 899-bb(1)(A).
4. **Documentation.** Finally, companies should keep in mind that they may need to demonstrate compliance with these requirements. To do so, ensure that your data security program is well documented and that the company policies reflect the security program.

The below table lists states with Reasonable Security Laws, states with Safe Harbor Laws, and other states that do or do not impose cybersecurity obligations on businesses.

States with "Reasonable" Cybersecurity Requirements	States with Cybersecurity Requirements but That Do Not Require "Reasonable" Cybersecurity	States with Safe Harbor Laws	States with No Cybersecurity Requirements
Alabama	Alaska	Connecticut	Iowa
Arkansas	Arizona	Ohio	Idaho
California	Colorado	Utah	Maine
Florida	Delaware		Minnesota
Hawaii	Georgia		Missouri
Illinois	Kentucky		Mississippi
Indiana	Louisiana		North Dakota
Kansas	Michigan		New Hampshire
Maryland	Montana		Oklahoma
Massachusetts	New Jersey		Pennsylvania
North Carolina	Wisconsin		South Carolina
Nebraska			South Dakota
New Mexico			Tennessee
Nevada			Washington
New York			West Virginia
Oregon			Wyoming
Rhode Island			
Texas			
Utah			
Vermont			
Virginia			
Washington, D.C.			

The Debevoise Data Portal is now available for clients to help keep track of their substantive cybersecurity requirements, as well as their state, federal, and international breach notification obligations. To subscribe to the Debevoise Data Blog, please click here.

The authors would like to thank summer associates Timothy Carey, Lexi Gaillard, and Kat McKay for their contributions to this blog post.

Jeremy Feigelson

Jeremy Feigelson is a Debevoise litigation partner, Co-Chair of the firm's Data Strategy & Security practice, and a member of the firm's Intellectual Property and Media Group. He frequently represents clients in litigations and government investigations that involve the Internet and new technologies. His practice includes litigation and counseling on cybersecurity, data privacy, trademark, right of publicity, false advertising, copyright, and defamation matters. He can be reached at jfeigelson@debevoise.com.

Avi Gesser

Avi Gesser is Co-Chair of the Debevoise Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy and artificial intelligence matters. He can be reached at agesser@debevoise.com.

Johanna Skrzypczyk

Johanna Skrzypczyk (pronounced "Scrip-zik") is a counsel in the Data Strategy and Security practice of Debevoise & Plimpton LLP. Her practice focuses on advising AI matters and privacy-oriented work, particularly related to the California Consumer Privacy Act. She can be reached at jnskrzypczyk@debevoise.com.

Alexandra P. Swain

Alexandra P. Swain is a Debevoise litigation associate. Her practice focuses on intellectual property, data privacy, and cybersecurity issues. She can be reached at apswain@debevoise.com.

Suchita Mandavilli Brundage

Suchita Mandavilli Brundage is an associate in Debevoise's Litigation Department. She can be reached at smbrundage@debevoise.com.

Parker Eudy

Parker Eudy is an associate in the Debevoise Litigation Department. He can be reached at pceudy@debevoise.com.

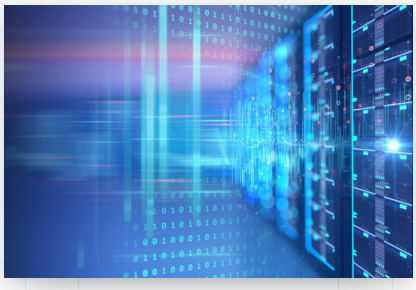
PREV POST

Podcast: Artificial Intelligence and Bias — Compliance & Legal Risk Podcast from Georgetown Law and EY

NEXT POST

OFAC's Ransomware Advisory Part 2 – How Banks Can Reduce Their Sanctions Risk for Client Cyber Ransom Payments

Related Posts



Data Minimization – Recent Enforcement Actions Show Why Some Companies Need to Get Rid of Old Electronic Records

MARCH 1, 2022

Four Takeaways from the SEC's Proposed Cybersecurity Rules

FEBRUARY 16, 2022

Webcast – Fireside Chat with NYDFS Cyber Chief Justin Herring

FEBRUARY 5, 2022